REMARKS

This Amendment is in response to the Office Action mailed on June 23, 2008. Claims 1-10, 12, 14-22, 35-37, 39, and 41-51 were pending in that action, and the Examiner rejected all of the claims. With this Amendment, claim 21 is amended, claims 35-37, 39, and 41-48 are cancelled, and the remaining claims are unchanged. Consideration and allowance of all pending claims are respectfully solicited in light of the following comments.

Specification Objection

On page 2 of the Office Action, the Examiner objected to the specification. The Examiner stated that the specification failed to provide antecedent basis for claims 35-37, 39, and 41-48. With this Amendment, claims 35-37, 39, and 41-48 have been cancelled. Applicant respectfully contends that the specification provides proper antecedent basis for all now pending claims. Applicant respectfully requests that the specification objection be withdrawn.

35 USC §101 Rejections

On page 2 of the Office Action, the Examiner rejected claims 35-37, 39, and 41-48 under 35 USC §101. With this Amendment, claims 35-37, 39, and 41-48 have been cancelled. Applicant respectfully contends that all now pending claims satisfy the requirements of 35 USC §101. Applicant respectfully requests that the 35 USC §101 rejections be withdrawn.

35 USC §112 Rejection

On page 3 of the Office Action, the Examiner rejected claim 1 under 35 USC §112 as being indefinite. The Examiner stated that it is not clear how the biometric device compares the session number to the record of the session number, because the record of the session number is stored in the computing device and not in the biometric device. Applicant respectfully contends that the Examiner is slightly misreading claim 1 and that this is what is causing the confusion.

The Examiner is correct in stating that the record of the session number is stored in the computing device and not in the biometric device. However, the Examiner is incorrect in reading claim 1 as stating that the biometric device compares the session number with the record of the session number. Very generally speaking, the session

number is generated by the computing device and sent to the biometric device. The biometric device then sends the session number back to the computing device where the computing device compares the session number to the record of the session number. The relevant language from claim 1 is below.

> "receiving a biometric information packet **from the biometric device**, decrypting it, and making a determination as to whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet, wherein making a determination comprises comparing a session number **received with or as part of the biometric information packet** to the record of the session number" (Emphasis Added.)

The above claim language shows that the biometric device is not comparing the session number to the record of the session number. The device that is doing the comparison is the computing device that receives the biometric information packet from the biometric device.

For at least the reasons listed above, Applicant respectfully contends that claim 1 is clear and satisfies the requirements of 35 USC §112. Applicant respectfully requests that the rejection be withdrawn. Applicant would also like to note that she would like to reduce the number of issues for appeal. Applicant respectfully requests that the Examiner let her know if any further information would be helpful to the Examiner to withdraw the §112 rejection.

35 USC §103 Rejections

Claim 1:

On pages 4-8 of the Office Action, the Examiner rejected claim 1 under 35 USC §103 as being unpatentable over Ting U.S. Pat. App. No. 2002/0174344 (hereinafter "Ting") in view of Michener U.S. Pat. No. 7,028,191 (hereinafter "Michener"). Applicant respectfully contends that claim 1 is patentable over the cited references for several reasons.

First, the Examiner cites Ting paragraph 13 as disclosing the claim 1 limitation of pre-establishing an encryption relationship between a computing device and a biometric device. The closest statement in Ting paragraph 13 is that "[t]he client includes a plug-in configured to receive a request for the candidate set of biometric data[.]" That statement does not disclose the claim 1 limitation. Claim 1 recites pre-establishing an encryption

relationship. Ting does not disclose an encryption relationship. The Ting reference simply states that the plug-in is configured to receive a request. There is nothing in Ting to suggest that this request is encrypted or that the configuring includes establishing an encryption relationship. Additionally, claim 1 further recites that the encryption relationship includes the computing device and the biometric device having separate but related encryption components. This further limitation was also rejected by the Examiner by Ting paragraph 13. As mentioned above, Ting paragraph 13 does not disclose an encryption relationship. It certainly does not disclose an encryption relationship that includes separate but related encryption components.

Second, on page 5 of the Office Action, the Examiner rejected the claim 1 limitation that the biometric device encryption component is implemented as firmware that decrypts information encrypted by the computing device encryption component. The Examiner provided two alternative bases for rejecting this limitation. The first basis was that the limitation is disclosed by Michener. In particular, the Examiner points to the crypto chip 44 and firmware keys 26 in Michener FIG. 1. Applicant respectfully disagrees with the Examiner's assertion. The Michener crypto chip and firmware keys do not decrypt information encrypted by a computing device encryption component. The crypto chip and firmware keys only encrypt informaton. This is stated in several section of Michener. For example, Michener column 4, lines 58-67, states that the crypto chip includes functionality to generate a signature and to encrypt data. Also for example, Michener column 7, lines 38-40, states that the firmware keys are used to generate maintenance keys. The Michener reference discloses that the decryption occurs at the Verification Decryption Server 32 that is part of the computing device and not part of the biometric device. Michener FIG. 1 shows that the Verification Decryption Server 32 ("VDS") is separate from the biometric device, Trusted Authorization Device 10. Michener column 12, lines 53-56, states that "[o]nce the VDS 32 accepts a transaction it completes the specified decryption and verification and returns the result before accepting another transaction."

On page 5 of the Office Action, the Examiner stated his second basis for rejecting the claim 1 limitation that the biometric device encryption component is implemented as firmware that decrypts information encrypted by the computing device encryption

component. The Examiner stated that it is well known in the art to implement encryption modules as firmware. Even if the Examiner's assertion is true, that does not make the claim 1 limitation unpatentable. Claim 1 goes beyond simply stating that the encryption component is implemented as firmware. Claim 1 recites that the firmware is related to the computing device encryption component and that it decrypts information encrypted by the computing device. Applicant does not believe that all of these limitations are well known in the art. The references cited by the Examiner teach away from this. For example, the most similar item in Ting is the Plug-in Module 132. As mentioned above, Plug-in Module 132 does not have a pre-established encryption relationship with the computing device. It is simply configured to receive a request from the computing device. Plug-in Module 132 also does not decrypt information sent by the computing device. Ting paragraph 26 states that it only encrypts information to send to a computing device. Additionally, Ting does not disclose implementing Plug-in Module 132 module as firmware. Plug-in Module 132 is part of client node 112. Ting paragraph 24 states that "client node 112 can be any computing device (e.g., a personal computer, set top box, wireless mobile phone, handheld device, personal digital assistant, kiosk, etc)[.]" All of these device are general use devices that do not have an encryption component implemented as firmware that is related to an encryption component in a computing device.

For at least the reasons discussed above, Applicant respectfully contends that claim 1 is patentable over the cited references considered individually or in combination. Applicant respectfully requests that the rejection be withdrawn and the claim allowed.

Claim 49:

On pages 16-18 of the Office Action, the Examiner rejected claim 49 as being unpatentable over Ting in view of Michener. Claim 49 includes several of the limitations discussed above in regard to claim 1. Applicant respectfully contends that claim 49 is patentable for the same reasons as discussed above. Claim 49 also includes additional limitations that are patentable.

First, very generally speaking, claim 49 recites that the computing device generates a session encryption key, that the computing device encrypts the session encryption key and sends the encrypted session encryption key to the biometric device,

and that the computing device receives a biometric information packet from the biometric device that is encrypted using the session encryption key. On page 17 of the Office Action, the Examiner states that Ting paragraphs 10, 25, 29-31, and 35-36 disclose these limitations. Applicant respectfully disagrees with that assertion. Perhaps the biggest difference between the claim 49 limitation and the cited sections of Ting is that Ting does not include a session encryption key. This means that Ting does not disclose that the computing device encrypts a session encryption key or that the computing device receives a biometric information packet that has been encrypted using the session encryption key. The most similar item that Ting discloses is a session code. The Ting session code is not a session encryption key. The session code is a simple identifier used by the computing device to track each biometric verification. For example, Ting paragraph 30 states that "[i]n response to the request for authentication, the identifying-characteristic generator module 124 ("ID generator") generates (step 208) an identifying characteristic, also referred to as a session code, to identify this particular transaction/session (e.g., response to the authentication request)." Also for example, Ting paragraph 34 states that "the session code is a random alphanumeric string and there is no reason for the client 112 to decipher this code because the client 112 does not use it, the client 112 simply has to retransmit the encrypted identifying characteristic back to the authentication server 108 with the candidate set of biometric data."

Another patentable limitation of claim 49 is that it recites the order of the steps. On page 17 of the Office Action, the Examiner states that Ting does not disclose the claim 49 step of encrypting the generated session packet, but that Michener does. Also, on page 17 of the Office Action, the Examiner states that the order of the steps is inherent. Applicant respectfully disagrees. Even if Ting and Michener in combination disclosed all of the claim 49 steps, which Applicant does not think that they do, it would not be necessary or inherent to combine them in the order recited in claim 49. For example, the session packet could be first encrypted when it is sent from the biometric device to the computing device, instead of first encrypting the session packet when sending it from the computing device to the biometric device as is recited in claim 49. Also for example, establishing an encryption relationship between the computing device and biometric device does not need to happen first as is recited in claim 49. The

encryption relationship could be established after the computing device sends the session packet to the biometric device.

For at least the reasons discussed above, Applicant respectfully contends that claim 49 is patentable over the cited references considered individually or in combination. Applicant respectfully requests that the rejection be withdrawn and the claim allowed.

Claims 2-10, 12, 14-22, and 50-51:

Claim 21 has been amended to correct a typographical error. Claims 2-10, 12, 14-20, 22, and 50-51 are unchanged. Applicant respectfully contends that these claims are allowable at least based on their dependence upon patentable independent claims. Applicant respectfully requests that the rejections be withdrawn and the claims allowed.

Conclusion

It is respectfully submitted that claims 1 and 49 are patentably distinguishable over the cited references considered individually or in combination. It is also respectfully submitted that claims 2-10, 12, 14-22, and 50-51 are patentable at least based on their dependence upon patentable independent claims. Accordingly, consideration and allowance of all pending claims are respectfully solicited. The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: /christopher l holt/

Christopher L. Holt, Reg. No. 45,844
Suite 1400
900 Second Avenue South
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax:(612) 334-3312

CLH:rkp